Description of Man-in-the-browser attacks against online banking and protection through SMS-based authentication

Audun Jøsang
February 2011
In the news

Online banks are vulnerable to attacks despite strong user authentication and encryption. PCs infected by ZeuS, SpyEye Trojans. Fake transactions through Man-in-the-browser attacks.

Advarer mot angrep mot nettbank-kontoer

Bankene har avdekket at kriminelle forsøker å nå norske nettbankkunders kontøer via trojanere, eller uønsket programvare, på kunders PC-er.

Foto: Illustrasjonsfoto: Colourbox

Bankene advarer mot et virus som gir kriminelle tilgang til kontøer i nettbanker. Flere tusen datamaskiner er allerede infisert, og et talls betalinger er forsøkt gjennomført.

HANS ERIK WEIBY
hans.ekir.wiebby@nrk.no

ZeuS and SpyEye Trojans
How they spread

• PCs get exposed to malware attacks when executing programs sent via phishing emails or found on websites.

• Unique attack signatures make AV software ineffective: Viruses evolve their "signature" for each infection or execution, and slip past AV software unnoticed, since AV software is based on known signatures.

• Probably around 50% of PCs are infected with some kind of malware.

• Hackers spend months targeting individual CEOs or businesses to loot their commercial bank accounts or to steal intellectual property.
Man-in-the-browser attacks

• Malware on a client PC waits until a customer is logged into their bank site, and then spawns a separate hidden window within the session to make fraudulent transactions. Strong user authentication and encryption provide no protection, because attack happens after the user is authenticated and inside the encrypted session.

• ZeuS and SpyEye Trojans: These are not individual viruses but are complete toolkits for sale on the Web. With a full suite of applications and developers around the world adding new capabilities all the time, these programs make it easy for thieves to mount very sophisticated man-in-the-browser attacks and keep them constantly changing.

• The fundamental vulnerability exploited by man-in-the-browser attacks against online banking is the lack of data/transaction authentication. It is not enough to have strong user authentication.
Man-in-the-browser attack scenario

1. Users specifies destination account and amount
2. Trojan changes destination account and amount
3. Transmits wrong transaction with attacker as destination
4. Bank transfers money to attacker
SMS authentication for preventing man-in-the-browser attacks

1. Specify destination account and amount
2. Transaction data transmission
3. SMS with authentication code, destination account and amount
4. View SMS
5. Verify transaction data in SMS
6. If transaction is correct, copy authentication code to browser
7. Transmit authentication code
8. Verify authentication code. If OK, execute transaction.
SMS with transaction details and authentication code

• SMS-based authentication provides verification of transaction data before execution.

• Verifying transaction details in SMS creates a cognitive load which reduces usability.

• With education and awareness this method provides both strong user authentication and strong data/transaction authentication.

Example mobile phone SMS message:

+61412345678
12345678 is your authentication code from National Australia Bank for Funds Transfer of $50 to BSB 123456 Account 123456789

Copy authentication code → Client terminal